AMENDMENTS TO THE CLAIMS

1-34 (cancelled)

35. (new) A method of authenticating a first electronic device to a first wireless network by a second electronic device storing an authentication key, each said electronic device having wireless communication capability independent of the other, comprising:

receiving an authentication challenge from said first wireless network at said first device;

forwarding said authentication challenge from said first device to said second device;

calculating an authentication response based on said authentication key at said second device;

forwarding said authentication response from said second device to said first device; and

transmitting said authentication response from said first device to said first wireless network to authenticate said first device but not said second device to said first wireless network.

36. (new) The method of claim 35 wherein said first device is a computing device and said first wireless network is a WLAN.

37. (new) The method of claim 35 wherein said second device is a cellular radiotelephone.

38. (new) The method of claim 35 wherein forwarding said authentication challenge and forwarding said authentication response occur across a communication interface connecting said first and second devices.

39. (new) The method of claim 38 wherein said communication interface is a wire or optical cable interface.

40. (new) The method of claim 38 wherein said communication interface is a wireless communication interface.

41. (new) The method of claim 40 wherein said wireless communication interface is an optical interface.

42. (new) The method of claim 40 wherein said wireless communication interface is a radio frequency interface.

43. (new) The method of claim 42 wherein said radio frequency interface is a BLUETOOTH interface.

44. (new) The method of claim 35 further comprising authenticating said first wireless device by said first wireless network based on said authentication response.

45. (new) The method of claim 44 wherein said authentication key comprises a shared key known to said first wireless network.

46. (new) The method of claim 45 wherein authenticating said first device by said first wireless network comprises:

using said authentication challenge and said shared key to compute an expected authentication response at said first network; and

comparing said expected authentication response with the actual authentication response received from said first device.

47. (new) The method of claim 44 wherein said authentication key is a private key known only to the second wireless device, and wherein a public key corresponding to said private is known to the first wireless network.

48. (new) The method of claim 47 wherein said first wireless network encrypts a data pattern using said public key to generate the authentication challenge, and wherein authenticating said first device by said first wireless network further comprises comparing the authentication response to the original data pattern used to generate the authentication challenge.

49. (new) The method of claim 48 wherein calculating an authentication response based on said authentication key comprises decrypting said authentication challenge to obtain the data pattern.

50. (new) The method of claim 35 further comprising:

forwarding said authentication response from said first wireless network to a second wireless network; and

authenticating said first device by said second wireless network based on said authentication response.

51. (new) The method of claim 50 further comprising:

sending an authentication result from said second wireless network to the first wireless network; and

providing or denying access for only the first device to the first wireless network based on said authentication result.

52. (new) The method of claim 51 wherein said authentication key comprises a shared key known to said second wireless network.

53. (new) The method of claim 52 wherein authenticating said first device by said second wireless network comprises:

using said authentication challenge and said shared key to compute an expected authentication response at said second wireless network; and

comparing said expected authentication response with the actual authentication response received from said first wireless network.

54. (new) The method of claim 51 wherein said authentication key is a private key known only to the second device, and wherein said private key has a corresponding public key that is known to the second wireless network.

55. (new) The method of claim 54 wherein said second wireless network encrypts a data pattern using said public key to generate the authentication challenge, and wherein authenticating said first device by said second wireless network further comprises comparing the authentication response to the original data pattern used to generate the authentication challenge.

56. (new) The method of claim 51 wherein said second network is a cellular wireless communication network.

57. (new) A non-provisioned electronic device having independent wireless communication capability, comprising:

a first interface to communicate with a wireless network;

a second interface to communicate with a provisioned electronic device having an authentication key;

a microprocessor connected to said first and second interfaces and programmed to:

forward an authentication challenge received from the wireless network via said first interface to the provisioned device via said second interface;

receive an authentication response from the provisioned wireless device via said second interface; and

forward the authentication response via said first interface to the wireless network to authenticate the non-provisioned device but not the provisioned device to the wireless network.

58. (new) The wireless device of claim 57 wherein the first interface is a WLAN interface.

59. (new) An electronic device provisioned with an authentication key comprising:

an interface to communicate with a non-provisioned electronic device;

an authentication unit connected to said interface and having a memory for storing the authentication key and a processor for performing calculations using said authentication key, said authentication unit being operative to:

receive an authentication challenge issued by a network from the non-provisioned device via said interface;

compute an authentication response using the authentication challenge and the authentication key; and

forward the authentication response via the interface to the non-provisioned device for use by the non-provisioned device to access the network;

whereby the provisioned device does not access the network.

60. (new) A method of authenticating a non-provisioned computing device having independent wireless communication capability to a WLAN using a provisioned cellular radiotelephone, comprising:

receiving an authentication challenge at the computing device from the WLAN;

forwarding the authentication challenge to the cellular radiotelephone;

receiving from the cellular radiotelephone an authentication response; and

forwarding the authentication response to the WLAN.